Notice of Allowability	Application No.	Applicant(s)	
	09/916,397	REDLICH ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *03/30/2006*.

2. ☒ The allowed claim(s) is/are *48-101,153-160 and 224-234*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert Kain on May 2, 2006.

The application has been amended as follows:

Claims

1 - 47. (cancelled)

48. (currently amended) A method for securing data in a computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, a ~~first and a second memory~~ plurality of memories respectively designated as a remainder store and ~~an~~ a plurality of extract ~~store~~ stores in ~~one or more computers~~ others of said plurality of computers, comprising:

establishing a group of security sensitive words, characters or icons for each of a plurality of security levels, each with a respective security clearance;

filtering data input from said data input computer and extracting said security sensitive words, characters or icons for each security level from said data to obtain extracted data and remainder data;

storing said extracted data in extract stores corresponding to respective security levels and said remainder data in ~~said extracted store and~~ said remainder store ~~, respectively~~ ; and,

accessing respective extract stores and permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a ~~predetermined~~ respective security clearance corresponding to a respective security level.

49. (currently amended) A method as claimed in claim 48 including defining a filter for a respective security level prior to said filtering step.

50. (original) A method as claimed in claim 49 wherein the step of defining the filter

includes the step of establishing said group of security sensitive words, characters or icons and the method includes one of storing said filter or destroying said filter after storing said extracted data.

51. (original) A method as claimed in claim 48 including encrypting one or both of said extracted data and remainder data prior to storing.

52. (original) A method as claimed in claim 51 wherein the step of permitting reconstruction includes decrypting one or both of said extracted data and remainder data.

53. (currently amended) A method as claimed in claim 48 ~~including establishing a plurality of security levels each with a respective security clearance, the step of establishing said security sensitive words, characters or icons including correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and the step of permitting reconstruction~~ including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security ~~clearance levels.~~ clearances.

54. (currently amended) A method as claimed in claim ~~49 wherein one of first and second computers are~~ 48 wherein said other computers are each respectively designated by a uniform resource locator (URL) and said storing utilizes said URLs. ~~for said first and second computers.~~

55. (currently amended) A method as claimed in claim ~~49 wherein said second computer is~~ 48 wherein said other computers are each respectively designated by a uniform resource locator (URL) and said data input computer and said other computers operates as a client in a client-server environment, ~~wherein said second computer operates as a server,~~ the method including sending said extracted data from said data input computer to said second

computer utilizing said respective URL and client-server protocol.

56. (currently amended) A method as claimed in claim 55 wherein said step of permitting reconstruction includes downloading said extracted data ~~from said second computer~~ utilizing ~~said URL and~~ said client-server protocol.

57. (currently amended) A method as claimed in claim ~~49 wherein said first and second computers are~~ 48 wherein said other computers are each respectively designated by respective uniform resource locators (URLs) and said data input computer operates as a client in a client-server environment, ~~wherein said first and second computers operate as respective servers,~~ the method including sending said remainder data and extracted data respectively from said data input computer to said ~~first and second~~ other computers utilizing ~~corresponding URLs and~~ client-server protocols.

58. (currently amended) A method as claimed in claim 57 wherein said step of permitting reconstruction includes downloading said remainder data and extracted data ~~respectively from said first and second computers~~ utilizing corresponding URLs and client-server protocols.

59. (original) A method as claimed in claim 58 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

60. (currently amended) A method as claimed in claim ~~49 wherein~~ 48 wherein a further one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

61. (currently amended) A method as claimed in claim ~~49~~ 48 including deleting said data input from said data input computer after the step of storing.

62. (currently amended) A method as claimed in claim ~~49~~ 48 including mapping said ~~first and second memory.~~ plurality of memories.

63. (previously amended) A method for securing data in a computer network with one or more security sensitive words, characters or icons and a plurality of security levels each with a respective security clearance, subsets of said security sensitive words, characters or icons being correlated with respective ones of said plurality of security levels, said computer network having a plurality of computers interconnected together, each of said plurality of computers having a memory therein, one of said plurality of computers designated as a data input computer, a first memory designated as a remainder store in said plurality of computers, and a corresponding plurality of memories in other ones of said plurality of computers designated as extract stores for respective ones of said plurality of security levels, comprising:

filtering data input from said data input computer for said plurality of security levels and extracting said security sensitive words, characters or icons for each of said security levels from said data to obtain extracted data for said security levels and remainder data;

storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store;

presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and,

permitting full or partial reconstruction of said data via said extracted data and remainder

data only in the presence of said predetermined security clearance after presentment of respective ones of said plurality of predetermined security clearances.

64. (previously amended) A method as claimed in claim 63 including defining a filter for said security levels prior to said filtering step.

65. (original) A method as claimed in claim 64 wherein the step of defining the filter includes the step of establishing a group of security sensitive words, characters or icons and the method includes one of storing said filter or destroying said filter after storing said extracted data.

66. (original) A method as claimed in claim 63 including encrypting one or both of said extracted data and remainder data prior to storing.

67. (original) A method as claimed in claim 66 wherein the step of permitting reconstruction includes decrypting one or both of said extracted data and remainder data.

68. (previously amended) A method as claimed in claim 63 wherein the step of storing stores remainder data in a different computer as compared with said data input computer and the step of presenting includes a plurality of presenting steps and the step of permitting reconstruction including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels after presentment.

69. (previously amended) A method as claimed in claim 63 wherein some of said plurality of computers are designated by uniform resource locators (URLs) and said storing utilizes said URLs.

70. (currently amended) A method as claimed in claim 63 wherein said data input computer operates as a client in a client-server environment ~~wherein said other ones of said~~

~~computers operate as a as a plurality of servers,~~ the method including sending said extracted data from said data input computer to said plurality of servers utilizing a URL and client-server protocol.

71. (previously amended) A method as claimed in claim 70 wherein said step of permitting reconstruction includes downloading said extracted data from said other ones of said computers utilizing said URL and said client-server protocol.

72. (currently amended) A method as claimed in claim 63 wherein said one and said other ones of said plurality computers are designated by respective uniform resource locators (URLs) and said data input computer operates as a client in a client-server environment, ~~wherein said one and said other ones of said plurality of computers operate as respective servers,~~ the method including sending said remainder data and extracted data respectively from said data input computer to said ~~one and said~~ other ones of said plurality of computers utilizing ~~corresponding URLs and~~ client-server protocols.

73. (currently amended) A method as claimed in claim 72 wherein said step of permitting reconstruction includes downloading said remainder data and extracted data respectively from said ~~one and said~~ other ones of said plurality of computers utilizing corresponding URLs and client-server protocols.

74. (original) A method as claimed in claim 73 including the step of encrypting and decrypting said remainder data and extracted data during sending and downloading.

75. (previously amended) A method as claimed in claim 63 wherein one of said computers is a reconstruction computer which includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of

reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays.

76. (previously amended) A method as claimed in claim 63 including deleting said data input from said data input computer after the step of storing.

77. (previously amended) A method as claimed in claim 63 including mapping said remainder store and said plurality of extract stores.

78. (currently amended) A method for securing data in a computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer, each of said plurality of computers having a memory therein, said plurality of computers including a ~~first~~ plurality of first designated computers each with a corresponding security level and security clearance and a second designated computer, ~~therein,~~ comprising:

establishing a group of security sensitive words, characters or icons for each said security level;

filtering data input from said data input computer and extracting said security sensitive words, characters or icons for each respective security level from said data to obtain extracted data for the respective security level and remainder data;

designating corresponding memory in said first designated ~~computer~~ computers as an extract store for each said respective security level and designating memory in said second computer as a remainder store;

storing said extracted data in said corresponding memory for each said respective security level and said remainder data in ~~said extracted store and~~ said remainder store; ~~, respectively;~~ and,

accessing respective corresponding memories and permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a ~~predetermined~~ respective security clearance corresponding to the respective security level.

79. (currently amended) A method as claimed in claim 78 wherein said step of designating includes storing a map of the ~~designated~~ corresponding memory.

80. (original) A method as claimed in claim 79 including storing said map in said data input computer.

81. (original) A method as claimed in claim 80 wherein the step of storing said map includes encrypting said map and the step of permitting reconstruction includes the step of decrypting said map.

82. (original) A method as claimed in claim 78 wherein said second computer is said data input computer and the step of filtering occurs thereat.

83. (original) A method as claimed in claim 78 including the step of encrypting one or both of said extracted data and remainder data.

84. (original) A method as claimed in claim 83 including the step of encrypting during the filtering step and prior to the storing step.

85. (original) A method as claimed in claim 84 including the step of decrypting during the reconstruction step.

86. (currently amended) A method as claimed in claim 78 including creating at least one filter for a respective security level and one of destroying or storing said filter after the filtering step.

87. (original) A method as claimed in claim 78 wherein one of said computers

includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

88. (original) A method as claimed in claim 78 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays on said one computer.

89. (original) A method as claimed in claim 78 including deleting said data input from said data input computer after the step of storing.

90. (previously amended) A method for securing data in a computer network with one or more security sensitive words, characters or icons and a plurality of security levels each with a respective security clearance, subsets of said security sensitive words, characters or icons being correlated with respective ones of said plurality of security levels, said computer network having a plurality of computers interconnected together, each of said plurality of computers having a memory therein, one of said plurality of computers designated as a data input computer, said plurality of computers including a first computer designated as a remainder store and a further plurality of computers designated as extract stores for respective ones of said plurality of security levels, comprising:

extracting said security sensitive words, characters or icons for said plurality of security levels from said data to obtain extracted data for respective security levels and remainder data;

storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store; presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and,

permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of respective ones of said predetermined security clearances after presentment thereof.

91. (previously amended) A method as claimed in claim 90 including designating a map of the extract stores and said remainder store..

92. (original) A method as claimed in claim 91 including storing said map in said data input computer.

93. (original) A method as claimed in claim 92 wherein the step of storing said map includes encrypting said map and the step of permitting reconstruction includes the step of decrypting said map.

94. (previously amended) A method as claimed in claim 90 wherein said data input computer filters the extracted data.

95. (original) A method as claimed in claim 90 including the step of encrypting one or both of said extracted data and remainder data.

96. (previously amended) A method as claimed in claim 95 including the step of encrypting prior to the storing step.

97. (original) A method as claimed in claim 96 including the step of decrypting during the reconstruction step.

98. (currently amended) A method as claimed in claim 94 including employing a

filter for said extracting step and one of destroying or storing said filter after the filtering step.

99. (original) A method as claimed in claim 90 wherein one of said computers includes a display fed from video memory having a plurality of frame memory segments, the reconstruction step including interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

100. (original) A method as claimed in claim 90 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the step of reconstruction including displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays on said one computer.

101. (original) A method as claimed in claim 90 including deleting said data input from said data input computer after the step of storing.

102 - 152. (cancelled)

153. (currently amended) A computer readable medium containing programming instructions for securing data in a computer network having a plurality of computers interconnected together, one of said plurality of computers designated as a data input computer and each of said plurality of computers having a memory therein, a ~~first and a second memory~~ plurality of memories respectively designated as a remainder store and ~~an~~ a plurality of extract ~~store~~ stores in ~~one or more~~ other computers in said plurality of computers, the programming instructions comprising:

establishing a group of security sensitive words, characters or icons for each of a plurality

of security levels, each level having a respective security clearance;

filtering data input from said data input computer and extracting said security sensitive words, characters or icons for a respective security level from said data to obtain extracted data and remainder data;

storing said extracted data in extract stores corresponding to respective security levels and said remainder data in ~~said extracted store and~~ said remainder store; ~~, respectively;~~ and,

accessing respective extract stores and permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of a ~~predetermined~~ respective security clearance corresponding to the respective security level.

154. (currently amended) A medium with programming instructions as claimed in claim 153 ~~including establishing a plurality of security levels each with a respective security clearance, correlating said plurality of security levels with subsets of said security sensitive words, characters or icons and permitting reconstruction~~ including the step of permitting a plurality of partial reconstructions of said data in the presence of respective ones of said plurality of security clearance levels.

155. (original) A medium with programming instructions as claimed in claim 153 including encrypting one or both of said extracted data and remainder data.

156. (original) A medium with programming instructions as claimed in claim 155 including encrypting during the filtering step and prior to the storing step.

157. (original) A medium with programming instructions as claimed in claim 156 including decrypting during the reconstruction step.

158. (currently amended) A medium with programming instructions as claimed in

claim 153 including employing a filter for the respective security level and one of destroying or storing said filter after the filtering step.

159. (original) A medium with programming instructions as claimed in claim 153 including deleting said data input from said data input computer after the step of storing.

160. (currently amended) A medium with programming instructions as claimed in claim 153 including mapping said ~~first and second memory.~~ said plurality of memories.

161 - 223. (cancelled)

224. (previously amended) An information processing system for securing data having one or more security sensitive words, characters or icons in a computer network, a plurality of security levels each with a respective security clearance, subsets of said security sensitive words, characters or icons being correlated with respective ones of said plurality of security levels, said computer network having a plurality of computers interconnected together, each of said plurality of computers having a memory therein, one of said plurality of computers designated as a data input computer, said plurality of computers including a first computer designated as a remainder computer store and a plurality of other computers designated as extract stores for respective ones of said plurality of security levels, the information processing system comprising:

a filter adapted to receive data input from said data input computer and to separate, from said data input, said security sensitive words, characters or icons into extracted data corresponding to respective ones of said plurality of security levels and remainder data;

a memory storage facility, coupled to said filter, for storing said extracted data in corresponding extract stores and said remainder data in said remainder store;

a security clearance control for each of said extract stores controlling access thereto only

in the presence of a predetermined respective one of a plurality of security clearances for each of said plurality of security levels; and

a compiler, coupled to said security control and said extract stores and said remainder store, for fully or partially reconstructing said data from said extracted data and said remainder data dependent upon access provided by respective ones of said plurality of security clearances.

225. (previously amended) An information processing system as claimed in claim 224 including means for mapping said extract stores and said remainder store, coupled to said memory storage facility.

226. (previously amended) An information processing system as claimed in claim 225 wherein said means for mapping creates a map for said corresponding extract stores.

227. (original) An information processing system as claimed in claim 226 including an encryptor coupled to said filter for encrypting said map and a decryptor coupled to said compiler for decrypting said map.

228. (previously amended) An information processing system as claimed in claim 224 wherein said filter is adapted to be removably coupled to said data input computer.

229. (original) An information processing system as claimed in claim 224 including an encryptor coupled to said filter for encrypting one or both of said extracted data and remainder data.

230. (original) An information processing system as claimed in claim 229 including a decryptor coupled to said compiler for decrypting one or both of said extracted data and remainder data.

231. (original) An information processing system as claimed in claim 224 including

means for deleting said filter, coupled to said filter.

232. (original) An information processing system as claimed in claim 224 wherein one of said computers includes a display fed from a video memory having a plurality of frame memory segments, the information processing system including said compiler adapted to be coupled to said video memory, said compiler having means for interleaving extracted data and remainder data into respective ones of said plurality of frame memory segments on said one computer.

233. (original) An information processing system as claimed in claim 224 wherein one of said computers includes a data display system with at least two separate but visually overlaid displays and at least two respective display interfaces, the information processing system including said compiler adapted to be coupled to said at least two display interfaces, said compiler having means for displaying said extracted data on one of said at least two displays and displaying said remainder data on another of said at least two displays on said one computer.

234. (previously amended) An information processing system as claimed in claim 224 including means for deleting said data input from said data input computer.

235 - 262. (cancelled)

2. The following is an examiner's statement of reasons for allowance: the prior art teaches filtering data based on security levels and storing the data and allowing full or partial reconstruction of data based on a respective security clearance. The prior art fails to teach storing only the extracted data for each security level at an extract store for each security level and storing the remainder data at a separate remainder store. Also the provisional obvious type double patenting rejections have been withdrawn because they were the only remaining rejections and this is the earliest of the applications pursuant MPEP 804(I)(B)(1).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. O'Flaherty et al (US 6253203) teaches the use of different stores for different security levels, but fails to teach any filtering of data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER